NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

Side-Channel Attack Project

Group Members:
Maria Mustafa Doola (U1720404J)
Goh Puay Hiang (U1820306A)

Introduction

Security is often, if not, the main concern for designers and end users when designing a cyber physical system. To ensure that critical and confidential information are only available to the eyes of authorised users, complex algorithms are implemented to encrypt these information so that they cannot be intercepted by unauthorised hackers. The reliability of the implemented cryptography algorithms depend upon how well-hidden the “key” to the decryption algorithm is from unauthorised users. Side-channel attacks have become a common methodology for unauthorised hackers to unveil the secret key and gain access to the protected system.

Side channel attacks operate by the attacker monitoring the system’s physical characteristics when the system is under normal operation and are implementing the programmed encryption algorithms as incorporated in its design. These physical characters include but are not limited to the pattern in power and current consumption, timing and electromagnetic radiation that is emitted by the system. Based on the information gathered, data analysis is performed to determine the hidden “secret key”.

This report focuses on the implementation of a correlation power analysis attack to determine the secret key to decrypt the contents of a system that employs the Advanced Encryption Standard. The report also focuses on common countermeasures that can be implemented to protect the system against side-channel attacks.

Correlation Power Analysis Attack

The system's power consumption can be observed from three sources: the dynamic power which is required to charge and discharge the capacitors in the system hardware, the leakage current which defines the small amount of power to be dissipated even when the system is idle as well as the system's power consumption when the hardware system undergoes a short circuit.

The cyber physical system's dynamic power consumption pattern is directly proportional to the number of transistors that switch state from logical 0 to logical 1 and vice versa. Similarly, a pattern for the leakage current can be observed based on the input provided to the physical system. With these observable patterns, attackers are able to decode the inputs to the system and obtain the "secret key" to decipher the system's "cipher text".

To perform a correlation power analysis attack, four important steps need to be carried out. Firstly, the system's power consumption pattern needs to be observed. The system is then required to encrypt several sets of plaintext to ciphertext with the system's power consumption trace observed when the encryption process is implemented. A divide and conquer approach is then adapted by dividing the secret key into subkeys. For each subkey guess, a modeled power consumption trace is generated with the guessed subkey and the plaintext. This power consumption trace is compared against the actual power consumption trace for that particular plaintext. The model trace that correlates most closely with the actual trace for the specific plaintext is assumed to be the best subkey guess. The full key is then obtained by gathering the best guesses for all the subkeys.

Pseudo Code of Correlation Power Analysis Code

The aim of this project is tp design and develop a program that would perform a correlation power analysis attack. Below is the pseudo-code for our program:

```
keysize = CPA.keysize
self.key = [None] * keysize

self.initTraceMatrix()
// initializes matrix of all the traces, plaintext and ciphertext

// loops for each of the 16 keys
for i in range(1,keysize + 1):
    self.initHypothesis_MCU8_AES128(i)
    // hypothesis the possible keypair
    self.findCorrelation()
    // find correlation between each possible combination and the power trace
    self.key[i - 1] = self.findKey()
    // compares computed correlation and finds the key with the highest correlation
retVal = {"key": strkey.strip(), "time": timetaken}
return retVal
```

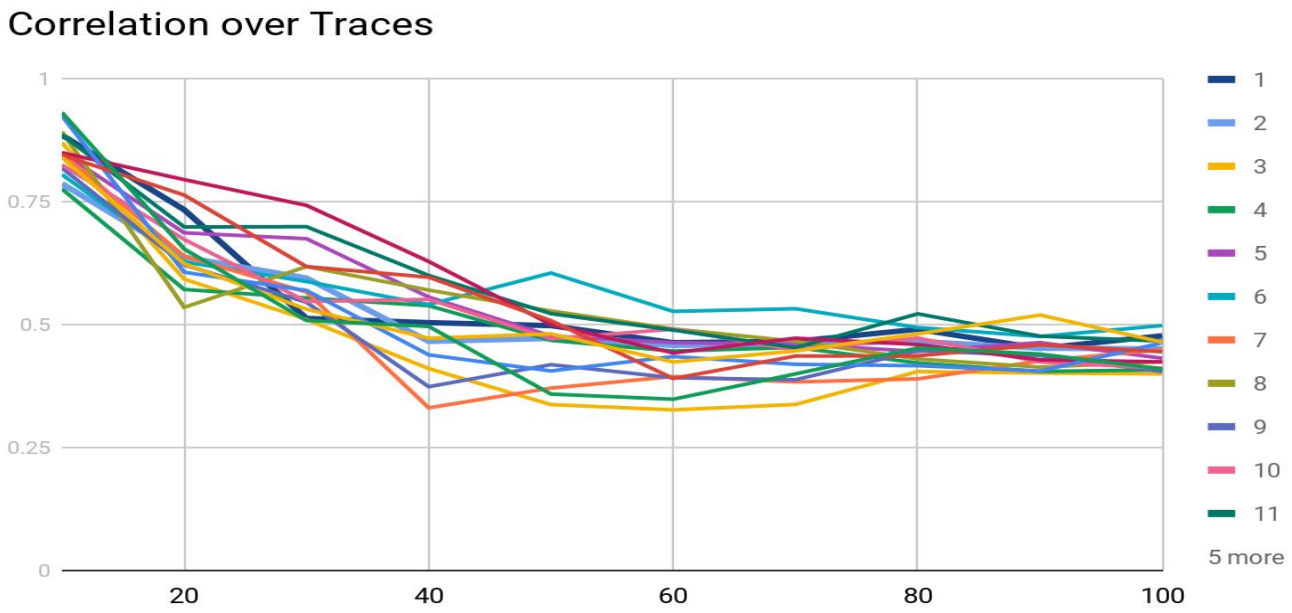
Our code for the project is available on Github in the link below:
https://github.com/GPHofficial/CX4055-Project/tree/master/CPA-Tool

Experimental Results

Below are the experimental results obtained from performing a correlation power analysis with our designed code:

- For 100 traces, plot the correlation of all possible key bytes and highlight the correlation of the correct key byte in red.
  The result of this plot graph can be found in the link below:
  https://github.com/GPHofficial/CX4055-Project/CPA-Tool/assignment31.ods

- Plot for "Correlation of the correct key byte vs number of traces". Let the number of traces run from 10 to 100 in steps of 10. This plot needs to be shown for all the 16 bytes of the key.



Raw data is available in the link below:
https://github.com/GPHofficial/CX4055-Project/blob/master/CPA-Tool/assignment32.csv

.

Countermeasures against Side-Channel Attacks

Here are some common countermeasures that can be implemented to reduce the possibility for a cyber physical system's confidentiality to be compromised by side channel attacks:

1) Hiding
   Attempts to side channel attacks can be reduced by hiding important information that can be leaked from side channels. Below are several measures that can be enforced to hide important data leaked from side channels:

   - A noise generator can alter the system's power and current consumption, timing and any other physical parameter to not correlate with the system's normal mode of operation by:
   - Implementing additional circuitry that would randomly add timing delays to the system's performance and dissipate current randomly to hide .
   - Ensure that the total power consumption observed from the system is constant regardless of the number of switching operations performed by the transistors within the system circuitry.
   - Add electromagnetic noise to the side channel during execution time to make it difficult for attackers to observe important data that may be leaked from the system's side channels.

   - Specialised logic units can be added to the cyber physical system during the design phase that could cause power or

timing delay that is independent of the secret key or the input data to prevent side channel attacks.

- Implementing asynchronous logic in the design phase of the system circuitry results in no clock and global synchronisation which are the basis for detecting information from side channels. This would result in many side channel attacks to fail.

- A system designed for low power dissipation can weaken the signals output from side channels, thus decreasing the difficulty of side channel attacks

- Side channels can be physically shielded to hide side channel leakages. This can be done by for example, applying an upper meta layer can prevent EM emission from observable side channels while the use of sound dampening emission can be used to prevent acoustic emission.

2) Masking

Attempts to side channel attacks can be reduced by masking the relationship between the data input and secret key with the information that is leaked to unauthorised users from side channels. Below are measures that can be implemented to the design of a cyber physical system to mask the relationship between leaked important information from side channels and the system's secret key:

- Gate-level implementation such as performing an XOR operation between the system's logical output and a pre-selected data value can mask the real data output from the system and prevent unauthorised users from tracing a relationship between the system output and the hidden key.

- Random data can be input to the system at planned time intervals to mask the relationship between the system's input and the information output from the system. However, this countermeasure could be difficult to implement as the circuitry's internal design of its logic units will be required to modify so that the system's functionality is not affected and generates the correct output.

3) Partitioning
   Below are countermeasures related to partitioning that can be implemented to reduce attempts to side-channel attacks:

   - Separating the memory locations allocated for plain-text and cipher-text.
   - The cyber physical system's infrastructure should be designed with the rails allocated for power supply, clock, network and testing to be separated for crypto-related operations and other functionalities performed by the system.

4) Physical Security
   Below are physical measures that can be implemented to reduce the possibility of a side-channel attack by denying unauthorised users access and possession of the system:

   - Acousting shielding can be used to protect a cyber physical system from acoustic emission attacks.
   - Secure construction zones can be added to the design of the system's design infrastructure to protect the system from electromagnetic emission attacks.